UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/064,943	08/30/2002	Bastian Pochon	CH920010045US1	3630

877 7590 05/03/2006

IBM CORPORATION, T.J. WATSON RESEARCH CENTER
P.O. BOX 218
YORKTOWN HEIGHTS, NY 10598

EXAMINER	
MIRZA, ADNAN M	

ART UNIT	PAPER NUMBER
2145	

DATE MAILED: 05/03/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/064,943	POCHON ET AL.	
	Examiner	Art Unit	
	Adnan M. Mirza	2145	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 August 2002*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-17* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-17* is/are rejected.

7)☒ Claim(s) *1-17* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *30 August 2002* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

1. Regarding claims 1,14,17, the phrase "and/or" renders the claim(s) indefinite because the claim(s) include(s) elements not actually disclosed (those encompassed by "and/or"), thereby rendering the scope of the claim(s) unascertainable. See MPEP § 2173.05(d).

Claim Objections

2. The numbering of claims is not in accordance with 37 CFR 1.126 which requires the original numbering of the claims to be preserved throughout the prosecution. When claims are canceled, the remaining claims must not be renumbered. When new claims are presented, they must be numbered consecutively beginning with the number next following the highest numbered claims previously presented (whether entered or not). The numbering of the claims should be made proper according to the MPEP.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vaidya (U.S. 6,279,113) and further in view of Spiegel (U.S. 6,954,765)

As per claims 1,14,17 Vaidya disclosed a method of normalization of traffic data that is simultaneously transferred to a network intrusion detection system (NIDS) and a monitored end-system located in a network in which packets of data are fragmented and reassembled, characterized in that the method comprises dynamically establishing and maintaining a normalization table into which information of received fragments and/or the topology of the network comprising the network intrusion detection system (NIDS) and the monitored end-system are entered and received packets of data are modified (col. 5, lines 5-26),

However Vaidya did not disclose in detail redirected or discarded in the event that ambiguities are detected when comparing information contained in the normalization table with information contained in the headers of the received data packets.

In the same field of endeavor Spiegel disclosed, "Valid handles for the copied sequence tables are written so that the copied sequence tables point to the appropriate original i.e. unaltered sequence tables and/or original fragments to complete the chains for the unaltered fragments.

The original sequence tables and fragments that have been copied are deleted from storage. The deletion may occur by various mechanisms (col. 9, lines 11-17). The updating procedures may involve replacing data, i.e. overwriting, removing data, i.e. truncating or discarding, or adding data, i.e. amending. Fig. 4 is a flow chart showing one method of updating. A particular that contains old data to be changed is identified. The old data may be the entire contents of the fragment or only part of the data contained within the identified fragment (col. 8, lines 51-57).

It would have obvious to one having one ordinary skill in the art at the time of the invention was made to have incorporated Valid handles for the copied sequence tables are written so that the copied sequence tables point to the appropriate original i.e. unaltered sequence tables and/or original fragments to complete the chains for the unaltered fragments. The original sequence tables and fragments that have been copied are deleted from storage. The deletion may occur by various mechanisms. The updating procedures may involve replacing data, i.e. overwriting, removing data, i.e. truncating or discarding, or adding data, i.e. amending. Fig. 4 is a flow chart showing one method of updating. A particular that contains old data to be changed is identified. The old data may be the entire contents of the fragment or only part of the data contained within the identified fragment as taught by Spiegel in the method of Vaidya to increase the perfomrace of the network by reducing network attack signature and so the network does have to spend more time creating new network attack signatures.

5. As per claim 2 Vaidya-Spiegel disclosed wherein fragments received are registered in the normalization table and forwarded to the end-system immediately thereafter in the event that

no conflict is detected with data of previously received fragments or discarded or redirected in case that a conflict is detected (Spiegel, col. 9, lines 11-17).

6. As per claim 3 Vaidya-Spiegel disclosed wherein for every incoming fragment, based on the content of the header fields IDENTIFICATION, PROTOCOL, SOURCE IP ADDRESS and DESTINATION IP ADDRESS, an identifier is built that allows a)to assign the fragment to data stored in the normalization table which belongs to earlier received fragments of an identified datagram d i and to update the normalization table with header data of the received fragment or, Win the event that no fragments of the identified datagram were received earlier, to establish a new entry for the identified datagram and update the normalization table with header data of the received fragment (Vaidya, col. 7, lines 24-31).

7. As per claim 4 Vaidya-Spiegel disclosed wherein for each datagram the header field FRAGMENT OFFSET is extracted and the length of the fragment data is calculated by means of the fields HEADER LENGTH and TOTAL LENGTH in order to establish the structure or information about the received section of the identified datagram without storing data of the identified datagram in said structure or normalization table (Vaidya, col. 8, lines 40-56).

8. As per claim 5 Vaidya-Spiegel disclosed wherein a partial and complete receipt of an App 1) identified datagram is recorded by means of a sliding bit-mask which is moved to an offset O i depending on the receipt of fragments, belonging to the identified datagram di, until

the offset O indicates receipt of all data contained I in the datagram data area of datagram di (Spiegel, col. 5, lines 43-64).

9. As per claim 6 Vaidya-Spiegel disclosed wherein an incoming fragment f with the offset f o and the length fv, by means of the sliding bit-mask covering a section of the expected datagram d with its length A , is I a) discarded in the event that O i > f O for the sliding bit-mask going in order or O i + A < f O + fv for the sliding bit-mask going in reverse order a) redirected to a processing unit with a sliding bit-mask of increased length A 2 , A 3 , ... in case that O i + A < f O + fv for the sliding bit-mask going in order or O i > f O for the sliding bit-mask going in reverse order (Spiegel, col. 5, lines 43-64).

10. As per claim 7 Vaidya-Spiegel disclosed wherein the registered data belonging to an identified datagram d i are cleared after the receipt of a corresponding ICMPmessage TIMEOUT EXCEEDED WHILE REASSEMBLY or after a time period T1 which is selected equal or slightly higher than the lifetime of the last fragment received and accepted (Vaidya, col. 6, lines 1-26).

11. As per claims 8,15 Vaidya-Spiegel disclosed wherein the distance and/or the path MTU to the end-systems in the network that are monitored by the network intrusion detection system (NIDS) are measured and stored in the normalization table before or upon the receipt of a data packet addressed to one of the monitored end-systems (Vidya, col. 3, lines 48-65).

12. As per claims 9,16 Vaidya-Spiegel disclosed wherein for a data packet, such as a datagram or fragment received, the TIME TO LIVE value and/or the path MTU measured for the addressed end-system are retrieved from the normalization table, and a)in the event that the content in the TIME TO LIVE field is lower than the required value, then it is replaced by the retrieved value and/or b)in the event that the path MTU is lower than the size of the data packet. the do not fragment FLAG, in case that it is set, is cleared (Vidya, col. 4, lines 18-27).

13. As per claim 10 Vaidya-Spiegel disclosed wherein the checksum is recalculated for all modified data packets which are forwarded to the addressed end-system (Spiegel, col. 2, lines 53-64).

14. As per claim 11 Vaidya-Spiegel disclosed wherein the distance and/or the path MTU to an end-system is measured by forwarding a UDP packet with the do not fragment flag DF set and a size corresponding to the maximum transfer unit MTU of the first link towards the addressed end-system, waiting for the return of an ICMP-message and a) in the event that an ICMP-message FRAGMENTATION REQUIRED BUT DF BIT SET is returned, sending a further UDP packet with reduced size to the addressed end-system and b)in the event that an ICMP-message PORT NOT REACHABLE is returned, computing the distance to the end-system and storing a required content for the TIME TO LIVE field as well as the probed path MTU in the normalization table (Vidya, col. 6, lines 1-26).

15. As per claim 12 Vaidya-Spiegel disclosed wherein an aging bit is added to all entries in the normalization table which is set whenever said entry is retrieved from the normalization table while, periodically after a time period T2, the aging bits of all entries are sequentially reset and entries with aging bits that are already reset are deleted (Spiegel, col. 8, lines 56-67 & col. 8, lines 1-8).

16. As per claim 13 Vaidya-Spiegel disclosed wherein, periodically after a time period T3, the distance and/or the path MTU to the end-systems corresponding to the entries stored in the normalization table are sequentially probed and, in case that values have changed, the normalization table is updated accordingly (Spiegel, col. 8, lines 27-34).

Conclusion

17. Any inquiry concerning this communication or earlier communication from the examiner should be directed to Adnan Mirza whose telephone number is (571)-272-3885.

18. The examiner can normally be reached on Monday to Friday during normal business hours. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jason Cardone can be reached on (571)-272-3933. The fax for this group is (703)-

746-7239. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

19. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for un published applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at (866)-217-9197 (toll-free).

AM

Adnan Mirza

Examiner

JASON CARDONE
SUPERVISORY PATENT EXAMINER